Entrust Master Control Command Shell

Quick Reference

Release 6.0.1 for Windows and UNIX

Performance monitoring commands

estat clear	clear performance counters
estat describe <name> | all	get description of one or all performance counters
estat print [-cont=<n>] [-dsigauges | -dsitrans]	display performance counters
[-cont]	display all gauges and counters at regular intervals
[-dsigauges | -dsitrans]	display gauges or counters at regular intervals

First-time initialization commands

init	initialize Entrust/PKI
subordinate make-subcert-req	generate a PKCS #10 certificate request to be sent to a superior CA
subordinate read-subcert	import a PKCS #7 response from a superior CA into Entrust/Authority

How to use this card

< >	indicate variables, for example, <subsys>
[ ]	indicate options, for example, [-ldap]
|	indicates either/or parameters, for example, all | list
+	indicates multiple values can be configured in one command

Security classes

Commands with no key icon are non-harmful commands not requiring access to the database. Require no authorization.

Non-harmful commands. Autologin must be enabled or you must be logged in to an active Entrust Master Control Command Shell session.

Commands requiring access to the database but not causing irreversible change. You must be logged in to an active Entrust Master Control Command Shell session.

Commands causing a policy change or update that may be irreversible. Requires one additional Master User password if policy has been set to require multiple authorizations. Otherwise, command shell may issue warning and yes/no prompt.

Getting help

help or ?	get list of all commands
help all | list | <cmd>	get help on all commands, list all commands, or get help on single command
apropos <regexp>	find commands related to regular expression
util errinfo <code>	describe error code
version	show release information

Logging in and out

login	log in to Entrust/Authority Master Control
logout	log out of Entrust/Authority Master Control
exit	stop the command shell
passwd <user>	change a Master User password

Tcl syntax tips

Basic syntax: command arguments

\   used to:
- keep commands and arguments together if they span more than one line
- quote special characters
- turn off meaning of symbols such as "", { }, [ ], $

" "   group words into single argument

{ }   group words into single argument; elements such as [ ] and $ are not interpreted as Tcl syntax

Tcl resources

Practical Programming in Tcl and Tk Third Edition, Brent B. Welsh, Prentice Hall PTR

Graphical Applications with Tcl & Tk Second Edition, Eric Foster-Johnson, M&T Books

http://www.scriptics.com

http://www.beedub.com/book

Additional documentation on Entrust Master Control Command Shell

See "Command-line interface for Entrust/Authority Master Control" in *Administering Entrust/PKI 6.0 on Windows* or *Administering Entrust/PKI 6.0 on UNIX*.

Visit our Web site at www.entrust.com.

Entrust TECHNOLOGIES

We Bring Trust to e-Business™

Entrust/Authority service commands

Command	Description
service autologin query | enable | disable	query, enable, or disable automatic login
service config <subsys> query | enable | disable | procs <n>	query, enable, or disable Entrust/Authority subsystem, or assign a number of processes to a subsystem
service start	start the service
service status	display the service status
service stop	stop the service

CA management commands

Command	Description
ca cert config (-lifetime <value> | -period <value>)+	change the lifetime and/or the private key usage period of the next CA certificate
-lifetime	set CA certificate lifetime (months)
-period	set private key usage period (percent of CA certificate lifetime)
ca cert export -binary | -pem {-x509 -cert | -pkcs7} | -wtls [-overwrite] <file>	export a CA certificate to file
-binary | -pem	export as binary or PEM
-x509 | -wtls	export as X.509 or WTLS certificate
-cert | -pkcs7	if X.509, return CA certificate, or certificate chain including superior CAs if current CA is subordinate
[-overwrite]	overwrite existing file
<file>	specify filename
ca cert get <sernum>	list detailed information about the CA certificate related to specified serial number
ca cert list	list all CA certificates
ca cert query	query CA certificate settings
ca cert revoke [-reason unspecified | cacompromise | superseded] [-text <value>] [-time [dd-mm[-yy[yy]].][hh:mm[:ss]]] <sernum>	revoke all CA and link certificates related to specified serial number
[-reason unspecified | cacompromise | superseded]	specify reason for revocation
[-text]	add a comment
[-time]	specify time when certificate was last known to be uncompromised
<sernum>	specify a certificate serial number
ca key config -alg RSA-1024 | RSA-2048 | DSA-1024	set the key type and size for the next CA key that is generated
ca key ec-params load <file>	load CA key elliptic curve parameters
ca key ec-params set-named <curve name>	set CA key elliptic curve parameters to a named curve

Command	Description
ca key ec-params write [-force] <ini file>	write CA key elliptic curve parameters to an initialization file
[-force]	overwrite an existing initialization file
<ini file>	pathname of initialization file
ca key move	move existing CA key to cryptographic hardware
ca key query	return the key type and size for the next CA key that is generated
ca key update	generate new CA certificate for new signing private key; save to software or hardware
ca keyrecover-all	set all clients up for key recovery
ca resynch-next-cert-serial	reset the certificate serial number
recover ca	recover CA profile

Policy management commands

Command	Description
policy authcode-dist enable | disable | query	enable, disable, or query authorization code distribution
policy auths enable | disable | query	enable, disable, or query Master User command authorization level
policy hasher md5 | sha1 | query	configure or query certificate hashing algorithm
policy proto-enc cast-80 | cast-128 | triple-des | query	configure or query protocol encryption algorithm
policy user-enc-keylen 1024 | 2048 | query	configure or query user encryption key length

Revocation list management commands

Command	Description
offlineARLs	update offline ARLs before they expire (if enabled)
rl count -crl | -arl	return a count of CRLs or ARLs
rl export [-pem | -bin] [-fn <fn>] (-crl <#>) | (-arl <#>) | (-cert <sn>) | -combined	return a CRL or ARL
[-pem | -bin]	return as PEM or binary
[-fn]	save the data to a file
-crl | -arl | -cert | -combined	specify CRL number, ARL number, certificate serial number, or combined CRL

Directory management commands

Command	Description
dsa diradmin <dn>	change the Directory Administrator DN
dsa passwd [-ldap] ca | diradmin	change the CA Directory Access password or the Directory Administrator password
[-ldap]	change password both in Directory and Entrust
ca | diradmin	specify either CA or Directory Administrator password
dsa pushrls	write CRLs and ARLs to Directory
dsa restore all | ca	restore CA data or all certificates to Directory

Certificate definition file commands

Command	Description
fcs export <file>	write certificate specifications from database to file
fcs import <file>	import specifications from certificate definition file into database

Security Officer commands

Command	Description
officer auths query | set <n>	get or change number of Security Officer authorizations required for sensitive operations
officer client-setting (query <name> | all) | (set <name> <value>)	get or set Security Officer client-side settings
officer create <dn>	create a Security Officer
officer list	list Security Officers
officer recover <dn>	recover a Security Officer

Database management commands

Command	Description
db backup incremental | full | query | config { -dir <backup-directory> | -keep <n> | -timer <incremental-period> <full-period> }+	perform, query, or configure full or incremental data backup
-dir	set backup directory
-keep	set number of backups to keep
-timer	set backup schedule
db get <var> | all	get specific or all configuration variables
db hw-protection disable	remove hardware-based database protection
db hw-protection enable -alg DES|Triple-DES|CAST-128	protect the database with a hardware-based key
db hw-protection query	query hardware-based database protection
db integrity validate | query | config { -timer <period> <notbefore> <notafter> }	perform, query, or configure automatic database validation
-timer	set database validation schedule
db lsaud [-d] [-f <outfile>] { <file>... | [-s [dd-mm[-yy[yy]].]<hh:mm[:ss]> | <day>] [-e date-time] }	list/check the audit file
[-d]	obtain complete description of activity
[-f]	write audit logs to file
<file>... | [-s] [-e]	view audit logs sent to file or specify start and end time for the log view
db re-encrypt	generate new random values for database encryption keys and re-encrypt database
db reports-timezone	update timezone information for reports
db set <var> <value>	set configuration variable